I. Isolamento

L'**isolamento** del sistema B è la prima fase critica per contenere l'attacco. Per farlo, si procede scollegando il sistema dalla rete, fisicamente o virtualmente, per evitare che l'attaccante possa continuare a compromettere altri sistemi o espandere l'infezione. In questa fase, utilizzo tecniche di **Network Segmentation** e **Zero Trust**, assicurandomi che i collegamenti di rete e qualsiasi accesso remoto siano bloccati. Inoltre, mi assicuro che non vi siano comunicazioni tra il sistema infetto e altri dispositivi della rete interna (A, C, D).

Questo isolamento non solo limita i danni ma consente anche di monitorare il comportamento del sistema compromesso senza che l'attaccante ne sia consapevole. Una volta isolato, viene eseguita un'analisi approfondita per comprendere la portata dell'intrusione e individuare eventuali altri dispositivi compromessi.

II. Rimozione del sistema B infetto

Dopo l'isolamento, il sistema B deve essere rimosso dalla rete. Prima di farlo, verifico se è possibile eseguire una **acquisizione forense** dei dati e della memoria RAM del sistema infetto, in modo da preservare le prove per eventuali indagini. Questo processo include:

1. **Spegnere le interfacce di rete**: Disabilito le interfacce di rete sul sistema B per evitare che l'attaccante possa riconnettersi.
2. **Backup dei log**: Prima della rimozione, estraggo tutti i log di rete, di sistema e di applicazione per l'analisi forense.
3. **Rimozione fisica o logica**: A seconda della gravità della compromissione, potrei rimuovere fisicamente il sistema, scollegando il server e posizionandolo in un'area sicura per l'analisi, o procedere con una disconnessione logica completa.

Questa fase è delicata, poiché deve essere eseguita in modo che l'attaccante non possa trarre vantaggio da eventuali tentativi di pulizia o auto-distruzione di prove (ad esempio, cancellazione dei file di log o disattivazione delle difese).

III. Differenza tra Clear, Purge e Destroy

Quando il sistema B è stato rimosso e l'attacco è stato contenuto, è necessario gestire in modo sicuro lo smaltimento delle informazioni sui dischi compromessi, garantendo che i dati sensibili non siano recuperabili.

- **Clear**: Questo processo implica una **cancellazione logica** delle informazioni tramite la sovrascrittura dei dati esistenti. È una tecnica di sanitizzazione utilizzata per rendere i dati meno accessibili, ma è possibile che siano recuperabili tramite tecniche avanzate di recupero dati. Ad esempio, un singolo passaggio di sovrascrittura può essere effettuato, ma non garantisce la totale inaccessibilità dei dati.
- **Purge**: Questo metodo è molto più sicuro rispetto al Clear, in quanto prevede l'uso di tecniche che rendono i dati **irrecuperabili anche con strumenti specializzati**. Un esempio comune è l'uso del **degaussing**, che smagnetizza i dischi rigidi, rendendoli illeggibili. Si possono usare anche algoritmi di sovrascrittura complessi o la disabilitazione elettronica permanente.
- **Destroy**: Questo è il metodo definitivo per eliminare ogni possibilità di recupero dei dati. Consiste nella **distruzione fisica** dei supporti, come la frantumazione dei dischi rigidi o lo smaltimento tramite inceneritori. Questo metodo è utilizzato per dati altamente sensibili o in casi in cui nessun rischio di recupero è accettabile.

Nel caso del sistema B compromesso, consiglio di adottare una combinazione di Purge e Destroy a seconda della sensibilità dei

dati conservati. Se i dischi contengono informazioni altamente riservate, la distruzione fisica dei dischi sarebbe l'approccio più sicuro. Tuttavia, per dati meno critici, il degaussing o altre tecniche di Purge possono essere appropriate.

FACOLTATIVO

Report di Analisi: Segnalazione di Problemi su Due Computer

A seguito delle segnalazioni da parte di due utenti circa problemi sui loro computer, ho proceduto all'analisi approfondita dei link associati alle possibili minacce. Sfruttando la piattaforma **any.run**, sono stati analizzati i comportamenti sospetti di file potenzialmente malevoli che potrebbero essere responsabili delle anomalie segnalate. Di seguito riporto i risultati delle analisi effettuate sui due link forniti e le azioni consigliate per mitigare i rischi legati all'attacco.

Analisi Link 1

L'analisi del primo link evidenzia che il file analizzato presenta comportamenti altamente sospetti. Ecco i principali risultati:

- **Connessioni di rete sospette**: Il malware tenta di connettersi a diversi **domini malevoli** e indirizzi IP associati ad attività di rete dannose. Questi domini sono spesso utilizzati dagli attaccanti per il controllo remoto o l'esfiltrazione di dati.
- **Modifiche al registro di sistema**: Il file tenta di modificare alcune chiavi di registro critiche per ottenere **persistenza** sul sistema, ovvero rimanere attivo anche dopo riavvii. Questo è un comportamento tipico di malware che cercano di mantenere il controllo a lungo termine del dispositivo infetto.
- **Esecuzione di comandi dannosi**: Durante l'analisi dinamica, il malware esegue **comandi potenzialmente pericolosi**, come l'esecuzione di script o l'avvio di ulteriori componenti

malevoli. Questi comandi possono essere utilizzati per scaricare altri tipi di malware o per compromettere ulteriormente il sistema.

Potenziale minaccia

Il comportamento osservato suggerisce che il malware sia un **trojan** o un **infostealer**, progettato per **rubare informazioni sensibili** (ad esempio, credenziali di accesso) e inviarle a un server di comando e controllo (C2). Questo tipo di malware potrebbe compromettere la sicurezza delle credenziali aziendali, dati finanziari o altre informazioni riservate.

Analisi Link 2

Il secondo link è anch'esso associato a un file sospetto, che presenta ulteriori segni di compromissione. Di seguito i principali dettagli dell'analisi:

- **Download di file aggiuntivi**: Il malware agisce come **downloader**, cercando di scaricare ulteriori componenti malevoli da un server remoto. Questo comportamento è tipico di malware modulari che espandono la propria funzionalità scaricando altri strumenti o payload malevoli, come ransomware o spyware.
- **Attività di rete anomala**: Sono state osservate diverse **connessioni a indirizzi IP non riconosciuti** e a **domini sospetti**. Queste connessioni possono essere utilizzate per inviare informazioni raccolte dal sistema o per ricevere comandi dall’attaccante.
- **Persistenza sul sistema**: Il malware cerca di creare **task pianificati** o di modificare chiavi di registro per garantire l’esecuzione automatica a ogni riavvio del sistema. Questo tipo di persistenza è spesso associato a spyware o botnet,

che hanno bisogno di eseguire attività di monitoraggio continuo o di controllo remoto.

Potenziale minaccia

Il secondo file potrebbe essere parte di una **campagna di phishing** o di un tentativo di installazione di **spyware**. Lo scopo principale di questo tipo di malware è rubare informazioni riservate (come dati di navigazione o credenziali) e inviarle a un server remoto per essere utilizzate in attacchi futuri o per la vendita sul dark web.

Azioni Consigliate

Sulla base delle due analisi, è evidente che i computer degli utenti sono stati probabilmente compromessi da **malware che puntano a rubare informazioni** o a installare altri componenti malevoli. Le azioni che consiglio per mitigare l'attacco e proteggere i sistemi aziendali sono le seguenti:

1. **Isolamento immediato dei sistemi compromessi**: I computer degli utenti devono essere immediatamente scollegati dalla rete per prevenire ulteriori danni e impedire la comunicazione con server malevoli.
2. **Acquisizione forense**: Prima di tentare qualsiasi rimozione del malware, è consigliabile effettuare una copia forense dei dischi e della memoria RAM dei sistemi infetti. Questo permetterà di preservare le prove dell'attacco e di svolgere un'analisi approfondita successiva.
3. **Rimozione del malware**: Dopo l'acquisizione forense, procedere con una **scansione approfondita** dei sistemi utilizzando strumenti anti-malware aggiornati. È consigliabile anche valutare il ripristino dei sistemi compromessi con nuove installazioni.
4. **Monitoraggio continuo**: Implementare strumenti di **monitoraggio del traffico di rete** per individuare e bloccare

eventuali ulteriori tentativi di connessione a domini o IP malevoli.

5. **Aggiornamento e patching**: Verificare che tutti i sistemi aziendali siano aggiornati con le ultime patch di sicurezza, in modo da ridurre la possibilità che il malware sfrutti vulnerabilità conosciute.
6. **Formazione del personale**: Educare i dipendenti riguardo alle tecniche di phishing e all'importanza di non aprire link o allegati sospetti. Implementare campagne di sensibilizzazione e simulazioni di phishing per migliorare la consapevolezza della sicurezza informatica in azienda.

In generale le due analisi dimostrano che i computer degli utenti sono stati infettati da **malware sofisticati** con l'obiettivo di rubare informazioni sensibili e mantenere l'accesso persistente ai sistemi. Le azioni di contenimento e rimozione devono essere eseguite con la massima urgenza per proteggere l'integrità della rete aziendale e dei dati sensibili.